

The opinion in support of the decision being entered today was **not** written for publication and is **not** binding precedent of the Board.

Paper No. 28

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte GLENN BENSON and MARKUS DICHTL

Appeal No. 2002-0617
Application 08/942,743

HEARD: February 13, 2003

Before BARRETT, FLEMING, and LEVY, **Administrative Patent Judges**.
FLEMING, **Administrative Patent Judge**.

DECISION ON APPEAL

This is a decision on appeal from the final rejection of claims 1, 3 through 8 and 10 through 46, all the claims pending in the instant application. Claims 2, 9 and 47 through 60 have been canceled.

The invention relates to mechanisms for protecting software against unauthorized copying. See page 1 of Appellants' specification. Appellants disclose that one of the problems of the prior art zero-knowledge protocol is protecting the private

key material. See pages 7 and 8 of Appellants' specification. Appellants disclose that one prior art way of protecting the private keying material is the use of smart cards. However, the problem still exists that if the customer's private keying material were to become unknowingly compromised then the private keying material could no longer be used in a meaningful way. See pages 8 and 9 of Appellants' specification. Appellants solve this problem by embedding a challenge means in the protected item of software. The challenge means has no access to the private keying material. The response means includes means for providing to the challenge means that the response means has access to the private keying material by interacting with the challenge means using a probabilistic proof scheme, and the challenge means comprises means for prohibiting a customer from using some or all the items of software unless the challenge means knows that the probabilistic proof is successful. See pages 9 and 10 of Appellants' specification.

Independent claim 1, present in the application, is reproduced as follows:

1. A computer system for preventing unauthorized use of software, comprising:

a protection mechanism for protecting software, the protection mechanism including challenge means for

providing a challenge associated with a protected item of software, and response means for responding to said challenge, to determine whether said response means has access to private keying material, wherein:

a) the challenge means has no access to said private keying material;

b) the response means includes means for proving that said response means has access to the private keying material by interacting with the challenge means using a probabilistic proof scheme,

c) the challenge means includes means for prohibiting a customer from using at least some of said item of software unless the challenge means determines from said probabilistic proof scheme that said response means in fact has access to said private keying material and thereby preventing unauthorized use of the software,

wherein said challenge means is embedded in said protected item of software.

References

The references relied on by the Examiner are as follows:

Linsker et al.	5,680,455	Oct. 21, 1997
	(filing date	Jul. 10, 1996)
Kanevsky et al.	5,774,525	Jun. 30, 1998
	(filing date	Aug. 14, 1997)
Hellman	5,872,917	Feb. 16, 1999
	(filing date	Oct. 8, 1997) ¹

¹We note that Hellman does not appear to be a valid reference applied against the Appellants in that the filing date is after the Appellants' filing date of Oct. 2, 1997.

Appeal No. 2002-0617
Application 08/942,743

Davis,² D. et al., "Cryptographic Randomness from Air Turbulence in Disk Drive", Advances in Cryptology: Crypto '94, Springer Verlag, pp 114-120.

Menezes,³ A. et al., Handbook of Applied Cryptography, CRC Press, pp 405-424, 1997.

Rosen, N.D., Examiner's Affidavit, June 11, 1999

Rejections at Issue

Claims 1, 3, 4, 10 through 16, 18, 25, 37 and 41 through 46 stand rejected under 35 U.S.C. § 103 as being unpatentable over Kanevsky in view of Menezes. Claim 5 stands rejected under 35 U.S.C. § 103 as being unpatentable over Kanevsky, and Menezes in view of Hellman. Claims 6 through 8 stand rejected under 35 U.S.C. § 103 as being unpatentable over Kanevsky, Menezes, and Hellman in view of Davis. Claim 40 stands rejected under 35 U.S.C. § 103 as being unpatentable over Kanevsky, and Menezes in view of Linsker. Claims 1, 3, 4, 10 through 18, 37 and 41 through 46 stand rejected under 35 U.S.C. § 103 as being

² The information for this reference was provided in the Information disclosure Statement filed June 4, 1998 (paper No. 5). We presume the year is 1994.

³ The Examiner has not established that this reference was published before the Appellants' October 2, 1997, because the published date just shows that it was published in 1997.

unpatentable over Rosen⁴ in view of Menezes. Claim 5 stands rejected under 35 U.S.C. § 103 as being unpatentable over Rosen and Menezes in view of Hellman. Claims 6 through 8 stand rejected under 35 U.S.C. § 103 as being unpatentable over Rosen, Menezes, and Hellman in view of Davis. Claim 40 stands rejected under 35 U.S.C. § 103 as being unpatentable over Rosen and Menezes in view of Linsker. Claims 19 through 24, 26 through 36, 38 and 39 stand rejected under 35 U.S.C. § 103 for the same reasons given with respect to claims 3 through 8, 10 through 16, 40 through 43, 45 and 46.

Rather than repeat the arguments of the Appellants or the Examiner, we make reference to the brief and the answer for the respective details thereof.

OPINION

For claims 19 through 24, 26 through 32, 33 through 36, 38 and 39, the Examiner does not clearly state the grounds for these rejections. We agree with Appellant's comments at the top of page 9 of the brief. We will not speculate as to how these

⁴Rosen refers to the Examiner's affidavit signed by Nicole David Rosen on June 11, 1999.

Appeal No. 2002-0617
Application 08/942,743

claims are rejected, therefore we find that these claims do not state a ground of rejection that can be reviewed. The rejection of claims 19 through 24, 26 through 36, 38 and 39 are reversed.

With full consideration being given to the subject matter on appeal, the Examiner's rejections and arguments of Appellants and the Examiner, for the reasons stated **infra**, we reverse the Examiner's rejection of claims 1, 3 through 8, 10 through 18, 25, 37 and 40 through 46 under 35 U.S.C. § 103.

We first will address the rejection of claims 1, 3, 4, 10 through 16, 18, 25, 37 and 41 through 46 under 35 U.S.C. § 103.

In rejecting claims under 35 U.S.C. § 103, the Examiner bears the initial burden of establishing a **prima facie** case of obviousness. **In re Oetiker**, 977 F.2d 1443, 1445, 24 USPQ 1443, 1444 (Fed. Cir. 1992). **See also In re Piasecki**, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984). The Examiner can satisfy this burden by showing that some objective teaching in the prior art or knowledge generally available to one of ordinary skill in the art suggests the claimed subject matter. **In re Fine**, 837, F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). Only if this initial burden is met does the burden of coming

forward with evidence or argument shift to the Appellants.

Oetiker, 977 F.2d at 1445, 24 USPQ at 1444. **See also Piasecki**, 745 F.2d at 1472, 223 USPQ at 788.

An obviousness analysis commences with a review and consideration of all the pertinent evidence and arguments. "In reviewing the [E]xaminer's decision on appeal, the Board must necessarily weigh all of the evidence and arguments." **Oetiker**, 977 F.2d at 1445, 24 USPQ2d at 1444. "[T]he Board must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the agency's conclusion." **In re Lee**, 277 F.3d 1338, 1344, 61 USPQ2d 1430, 1434 (Fed. Cir. 2002). With these principles in mind, we commence review of the pertinent evidence and arguments of Appellants and Examiner.

Appellants argue that neither Kanevsky nor Menezes teaches or suggests the protection of software from unauthorized use by having the challenge means embedded in the protected item of software that is distributed to the user and others. Appellants argue that the challenge means prevents the software from being used without authorization and has the seller's public key embedded in it. The seller obtains the buyer's public key and

embeds it into a keyfile that is sent to the buyer and installed by the buyer, where a probabilistic proof is carried out to permit the buyer to use the software in which the buyer already has in their possession. Appellants argue that neither Kanevsky nor Menezes teaches or suggests to those skilled in the art to the Appellants' claimed software protection scheme. See pages 10 through 12 of Appellants' brief.

As pointed out by our reviewing court, we must first determine the scope of the claim. "[T]he name of the game is the claim." **In re Hiniker Co.**, 150 F.3d 1362, 1369, 47 USPQ2d 1523, 1529 (Fed. Cir. 1998). In addition, claims are to be interpreted as the terms reasonably allow. **In re Zletz**, 893 F.2d 319, 321, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989).

We note that independent claim 1 (as well as claims 3, 4, 10 through 16, 37 and 41 through 46 due to their dependency on claim 1) recites:

computer system for preventing unauthorized use of software, comprising: a protection mechanism for protecting software, the protection mechanism including challenge means for providing a challenge associated with a protected item of software, . . . wherein: a) the challenge means has no access to said private keying material; . . . c) the challenge means includes means for prohibiting a customer from using at least some of said item of software unless the challenge means determines from said probabilistic proof

scheme that said response means in fact has access to said private keying material and thereby preventing unauthorized use of the software, wherein said challenge means is embedded in said protected item of software.

Similarly, we note that independent claim 18 (as well as its dependent claim 25) recites:

A method for protecting an item of software, comprising the steps of: associating challenge means with said protected item of software, and accessing private keying material by a response means, wherein a) the challenge means has no access to the private keying material, b) the challenge means prohibiting a customer from using at least some of said items of software unless the challenge means knows that said probabilistic proof is successful.

Thus, we agree that the claims are of such scope to include protecting an item of software in which the challenge means is embedded in the software which has no access to the private keying material.

We find that Kanevsky does not address protection of the software. Kanevsky relates to authorizing access to banking or credit accounts, pay per view video services or the alike. See column 1, lines 10 through 23 of Kanevsky. Kanevsky teaches that figure 1 is a functional block diagram of the secure access control system in a service provider network. See column 2, lines 40 through 44. Kanevsky teaches that upon determining that the user is an authorized individual, the authentication system 10 forwards the input data to the requested service provider

network 2 via communication links 14 for processing the transaction. Upon determining that the user is not an authorized individual, the authentication system 10 may forward the data indicating such to the requested service provider network 2 program over the communication link 14. See column 3, lines 8 through 15 of Kanevsky. We find no teaching or suggestion of distribution of software products by Kanevsky, nor do we find a teaching or suggestion of initial distribution of the software in which a challenge means is embedded within it.

We find that Linsker does teach a zero-knowledge identification protocol. However, we fail to find that the general teaching of Linsker teaches or suggests the Appellants' claimed invention of preventing unauthorized use of software by providing a challenge means which has no access to private keying material and wherein the challenge means is embedded in the protected item of software. Therefore, we will not sustain the Examiner's rejection of claims 1, 3, 4, 10 through 16, 18, 25, 37 and 41 through 46 as being unpatentable under 35 U.S.C. § 103 over Kanevsky in view of Menezes. For the rejections of claims 5 through 8 and 40 relying additionally on Hellman, Davis and Linsker, we find that the Examiner has relied only on Kanevsky

and Menezes for the above discussed limitations. Therefore, we will not affirm these rejection as well.

We now turn to the rejections of claims 1, 3, 4, 10 through 18, 37 and 41 through 46 under 35 U.S.C. § 103 as being unpatentable over Rosen in view of Menezes. Appellants disagree with the Examiner's statement that the computer game called "Pipe Dream" includes a response means that does not have access to private keying material. See page 17 of the brief. Appellants argue that the "Pipe Dream" game does not teach or suggest a response means including means for proving that the response means has access to the private keying material. See page 18 of Appellants' brief. Appellants further dispute the Examiner's statements that the "Pipe Dream" uses a code wheel. Thus, Appellants have placed facts in dispute.

When determining obviousness, "the [E]xaminer can satisfy the burden of showing obviousness of the combination 'only by showing some objective teaching in the prior art or individual to combine the relevant teachings of the references.'" **In re Lee**, 277 F.3d 1338, 1343, 61 USPQ2d 1430, 1434 (Fed. Cir. 2002), **citing In re Fritch**, 972 F.2d 1260, 1265, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992). "Broad conclusory statements regarding the teaching of multiple references, standing alone, are not

'evidence.'" **In re Dembiczak**, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617. "Mere denials and conclusory statements, however, are not sufficient to establish a genuine issue of material fact."

Dembiczak, 175 F.3d at 999, 50 USPQ2d at 1617, **citing McElmurry v. Arkansas Power & Light Co.**, 995 F.2d 1576, 1578, 27 USPQ2d 1129, 1131 (Fed. Cir. 1993).

In addition, our reviewing court requires the PTO to make specific findings on a suggestion to combine prior art references. **Dembiczak**, 175 F.3d at 1000-01, 50 USPQ2d at 1617-19. Our reviewing court states further that the "factual question of motivation is material to patentability, and could not be resolved on subjective belief and unknown authority."

We find that the Examiner has not rebutted Appellants' assertions as to the lack of a code wheel. Some objective teaching in the prior art is required. Appellants have placed in dispute the facts set forth in the Examiner's affidavit. The "Pipe Dream" game appears to be available to the Examiner so that the Examiner can establish exactly what the "Pipe Dream" is through the use of objective documentary evidence. The Board must assure that the requisite findings are made based on the evidence of record. Therefore, we will not sustain the

Appeal No. 2002-0617
Application 08/942,743

Examiner's rejection of claims 1, 3, 4, 10 through 18, 37 and 41 through 46. Furthermore, we will not sustain the rejection of claims 5 through 8 and 40 for the same reasons.

In view of the foregoing, we have not sustained these rejections of claims 1 3 through 8 and 10 through 46.

REVERSED

LEE E. BARRETT)	
Administrative Patent Judge)	
)	
)	
)	BOARD OF PATENT
MICHAEL R. FLEMING)	
Administrative Patent Judge)	APPEALS AND
)	
)	INTERFERENCES
)	
STUART S. LEVY)	
Administrative Patent Judge)	

MRF:pgg
Schiff Hardin & Waite
Patent Department
6600 Sears Tower
Chicago, IL 60606-6473

Appeal No. 2002-0617
Application 08/942,743